![Software Engineering Institute | Carnegie Mellon University]

Creating Centralized Reporting for Microsoft Host Protection Technologies: The Enhanced Mitigation Experience Toolkit (EMET)

Craig Lewis
Joseph Tammariello

August 2016

http://www.sei.cmu.edu

Table of Contents

List of Figures

Acknowledgments

Special thanks to our leadership within the Office of the Chief Information Officer for supporting this work.

Abstract

Host protection strategies, such as enabling anti-exploitation features, can be effective in protecting Windows endpoints from compromise. Microsoft offers a tool to assist in this area and is provided at no cost. The Enhanced Mitigation Experience Toolkit (EMET) is a utility that helps to prevent the exploitation of software vulnerabilities.

EMET can be effective in safeguarding organizations from compromise by malicious actors. The configuration of EMET can be controlled centrally by enterprise system administrators using Group Policy. While centralized management capability is built into the tool, centralized reporting capabilities are not, creating a challenge when it comes to real-time situational awareness, metrics gathering, troubleshooting, and reporting. This report presents methods by which systems administrators and/or information security personnel can create a centralized reporting console using native Windows capabilities and the Splunk machine data analysis engine.

1 Introduction

Anti-exploitation capabilities are a possible component of a defense-in-depth strategy to protect systems from compromise by malicious actors. Microsoft provides a cost-effective solution to help system administrators in this area. The Enhanced Mitigation Experience Toolkit (EMET), while not included with Windows at the time of this writing, is offered at no cost by Microsoft and can provide additional protection to vulnerable software.

While EMET offers valuable protection on enterprise endpoints and has centralized configuration management capabilities through the use of Group Policy, it lacks a centralized reporting capability. Events recorded by EMET are written to a Windows event log on the host but are not standardly recorded in a dashboard or console for system administrators or information security staff to review. Alerts and metrics from security events provide situational awareness and insights into activities happening on the corporate network. To understand how systems are being attacked and protected by EMET, administrators must create their own reporting strategy.

This report presents methods to centrally report EMET alerts generated on endpoints to IT professionals. Citing a variety of tools and strategies—from Group Policy and native event forwarding capabilities to the Splunk analysis engine—this report describes approaches to gaining awareness and building a reporting strategy relevant to the deployment of EMET in a centrally managed environment. The strategies discussed in this report are broadly applicable and can be applied singularly to EMET or any other application that logs events but has no centralized reporting capability.

1.1 Audience and Structure of This Report

This report is intended for system administrators and information security professionals who are interested in centralized reporting of EMET events recorded in local logs of enterprise endpoints. We assume that readers are familiar with software deployment and Windows event logs and have deployed or are considering the deployment of EMET. The deployment and management of EMET itself is outside of the scope of this report.

2 Protecting Endpoints and the Organization: The Case for Reporting on EMET

The protection of host systems is an important component of the comprehensive defensive posture of an organization. Common host-based strategies such as using anti-virus software and timely patching are helpful, though they offer little or no protection for attacks using specialized malware or unpatched "zero-day" exploits.

2.1 Benefits of Using EMET for Anti-Exploitation Mitigations

Application whitelisting and other host-hardening strategies can be beneficial in making hosts more resilient to computer network exploitation, though software that- *is* permitted to run by application control solutions such as Microsoft's AppLocker can still be exploited. EMET provides an additional layer of protection by restricting techniques commonly used by malicious actors. EMET can help to protect against the successful exploitation of vulnerabilities in software created by Microsoft or by third parties.

EMET provides a number of benefits to organizations using Microsoft Windows:

- EMET can serve as a mitigation in cases where a patch is not yet available or cannot be deployed, no alternate mitigation exists, or against zero-days using a variety of exploit techniques.
- EMET is provided by Microsoft at no cost.
- Configurations may be controlled centrally using Group Policy.
- Events are recorded to host event logs by default.

2.2 Why Centralized Notification and Reporting Matters

As described, EMET can be helpful in a layered defensive strategy for protecting endpoints. However, relying on the protections these technologies provide without investigating the results of their actions is not enough. Trusting that EMET is providing protections and not analyzing logged events is insufficient for situational awareness about what is happening on the network, the nature of the threat to individuals and the organization, and for continuous improvement in overall network defense. In their paper *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*, Hutchins, Cloppert, and Amin describe the importance of understanding unsuccessful intrusion attempts this way:

> *Equally as important as thorough analysis of successful compromises is synthesis of unsuccessful intrusions. As defenders collect data on adversaries, they will push detection from the latter phases of the kill chain into earlier ones. Detection and prevention at pre-compromise phases also necessitates a response. Defenders must collect as much information on the mitigated intrusion as possible, so that they may synthesize what might have happened should future intrusions circumvent the currently effective protections and detections* [Hutchins 2010].

EMET logs the actions taking place on hosts though it lacks a native capability for systems administrators and network defenders to centrally view and analyze events. By understanding the event logging of EMET and leveraging a centralized auditing and analysis solution, network defenders can more easily gain situational awareness and reduce the time and effort necessary to understand and respond to these events. Defenders may also use this information to better protect against future events.

3 EMET Logging Considerations

3.1 Log Consolidation Strategy

The strategy used for collecting and alerting on events of interest is dependent on the needs and resources of the organization. A host-monitoring service using third-party agents or a security information and event management (SIEM) solution may potentially be leveraged for the purposes of collecting, alerting, and reporting EMET events.

However, smaller organizations may not be able to invest in a SIEM or other agent-based third-party monitoring solution. In addition, an organization may choose to limit the number of agents installed on hosts or have other restrictions related to the installation of additional software. Those organizations may benefit from using native Windows capabilities for forwarding events and event log subscriptions. Detailed information on Windows event log monitoring—including event collection—is available in the National Security Agency (NSA) Information Assurance Directorate document *Spotting the Adversary with Windows Event Log Monitoring*.[1] Microsoft also publishes documentation on the Windows Event Collector capability, including source and collector initiated subscriptions.[2]

3.2 EMET Events

A Windows service called "Microsoft EMET Service" is set to start automatically after EMET is installed. It reports EMET events to the Windows Event Log. Events for EMET are recorded in the Application Log with an event source of *EMET*. These events are detailed in the *EMET User Guide*, part of the EMET installation available from Microsoft.[3]

It is important to note that some mitigations may not be fully logged by EMET if they are native operating system protections or enabled as system-wide mitigations. Examples include Mandatory Address Space Layout Randomization, Data Execution Prevention, and Structured Exception Handling Overwrite Protection.[4]

---

[1]   See https://www.iad.gov/iad/library/reports/spotting-the-adversary-with-windows-event-log-monitoring.cfm

[2]   See https://msdn.microsoft.com/en-us/library/windows/desktop/bb427443(v=vs.85).aspx

[3]   See http://www.microsoft.com/emet

[4]   See https://www.microsoft.com/en-us/download/details.aspx?id=50802 for more information about the *Enhanced Mitigation Experience Toolkit 5.5 User Guide*

4 Example Implementation Using Windows Event Collector and Splunk

This report describes a solution that uses a combination of Windows event collection and Splunk, as a SIEM/reporting solution, to report on events logged by hosts with EMET installed and configured. Splunk is an indexing solution for the analysis of machine data. Splunk was chosen for this report since a free version is available and may be used to quickly index and search large quantities of data. Splunk has free, cloud, and enterprise versions. Some differences exist in the features of these versions;[5] differences include restrictions on the amount of data indexed per day and the ability for real-time alerting. While a Splunk forwarding agent may be installed and configured on endpoints to collect some or all events, one can also use subscriptions and Windows Event Forwarding to collect only the events of interest from hosts and then index them with Splunk on the Event Log Subscription Server. This approach also uses a Windows capability included with the operating system in conjunction with the free EMET utility.

Using subscriptions and native event forwarding capabilities may allow for faster implementation of a centralized reporting capability, limit the number of events being indexed on by the free Splunk license, or be used as a proof of concept implementation of forwarding all logs. It may also provide validation for expanding log indexing capability and incurring the additional expense associated with expanded log collection and analysis capabilities.

4.1 Configure Windows Event Collection

Windows Event Collection can be configured on the endpoint directly or by Group Policy. In addition, subscriptions can be configured as collector initiated (pull) or source computer initiated (push). As this report is geared toward implementation in an enterprise setting where systems are likely to be in the same authentication domain, we discuss configuration using GPO and source-computer-initiated subscriptions.

4.1.1   About Subscriptions

Source-initiated subscriptions allow one to define a subscription on an event collector computer and then scope that subscription to a group of computers, (e.g., domain computers). Multiple remote event source computers can then be set up (using a Group Policy setting) to forward events to the event collector computer. This differs from a collector-initiated subscription; with collector-initiated subscriptions one cannot use computer groups when defining the source computers, only individual computers.

---

[5]   See http://www.splunk.com/en_us/products/splunk-enterprise/free-vs-enterprise.html

4.1.2   Configure a Collection Server and Subscription

Using a server host running Windows Server 2008 R2 or later, ensure that the Windows Event Collector service is enabled and set to start automatically. Also ensure that all host-based and network firewalls allow communications between Windows endpoints and hosts acting in the collection service role.

Define a subscription in the Event Viewer. Select *Subscriptions* and click *Create Subscription...* from the *Actions* panel. After entering a subscription name and optional description, change the subscription type to *Source computer initiated*. At this point, enter the computer group(s) you wish to be enrolled in the subscription and click OK to return to the *Subscription Properties* window.

In the *Subscription Properties* window, click "*Select Events...*" in the *Events to collect:* section and click the *XML* tab. After checking the *Edit query manually* checkbox and accepting the warning, enter the following:

```
<QueryList>
 <Query Id="0" Path="Application">
  <Select Path="Application">*[System[Provider[@Name='EMET'] and (Level=2)]]</Select>
 </Query>

</QueryList>
```

This query will select events of the *source* EMET from the *Application* log with the *Event ID,* 2.

Click OK to save the Query Filter and click OK again to save the subscription.

To receive notification for all forwarded events immediately, it may be advisable to change the DeliveryMaxItems setting to a value of 1 using the wecutil.exe[6] command.

4.1.3   Create a Group Policy Object to Configure Event Forwarding

After defining a subscription on the collection server, a Group Policy Object (GPO) can be created and deployed in order to direct targeted computers to the collection server. Once the computers connect to the collection server, the subscription will declare which events should be forwarded.

Ensure that the WinRM service is enabled on the endpoints that will be forwarding events. Open a GPO editor and navigate to the *Computer Configuration\Policies\Windows Settings\Security Settings\System Services\Windows Remote Management (WS-Management)* setting. Define the policy setting and select *Automatic* as the service startup mode.

For the policy settings to be applied to client systems, open a GPO editor and navigate to the *Computer Configuration\Policies\Administrative Templates\Windows Components\Event Forwarding* container. Edit the Configure target Subscription Manager setting. Enable the setting to

---

[6]   See technet.microsoft.com/en-us/library/cc753183.aspx

Configure target Subscription Manager and enter the IP or fully qualified domain name of the collection server by clicking the *Show...* button next to Subscription Managers. If using multiple event collectors, one may enter multiple fully qualified domain names or IPs.

Under the *Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management/WinRM Service* container, enable the setting for *Allow remote server management through WinRM* and enter the IP address of your collection server.

4.2 Forward Collected Events to Splunk

With EMET logs from endpoints forwarding to the collection server, the next step is to send those logs from the collection server to Splunk for analysis. While the logs may be reviewed using the Event Viewer on the collection server, the analysis capabilities of that tool are limited. To analyze the data in Splunk, install the Splunk Universal Forwarder on the collection server and configure it to send logs from the Forwarded Events log to a Splunk indexer.[7] When creating a subscription, the default location of forwarded log events is the Forwarded Events log. A sample stanza that could be used in the Splunk inputs.conf file on the collection server (this file defines which logs are to be send to Splunk) could include the following:

```
[WinEventLog://ForwardedEvents]
disabled = 0
renderXml = 1
evt_resolve_ad_obj = 1
```

The above stanza instructs the Splunk Universal Forwarder to monitor the Forwarded Events log and to resolve any Active Directory objects such as username and computername. Sending the events in XML format allows for facilitated extraction of information in Splunk to aid in the creation of useful Splunk queries.

Sample EMET Event:

```
EMET version 5.5.5871.31892
EMET detected EAF+ mitigation and will close the application: IEXPLORE.EXE

EAF+ check failed:
 Application     : C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE
 User Name       : DOMAIN\user
 Session ID      : 1
 PID             : 0x1348 (4936)
 TID             : 0xF90 (3984)
 Module          : SOMEDLL.dll
 Mod Base        : 0x11630000
 Mod Address     : 0x11642E99
 Mem Address : 0x76F501A4
```

---

[7]   See http://docs.splunk.com/Documentation/Splunk/latest/Data/MonitorWindowseventlogdata

4.3 Analyzing Events Using Splunk

Once EMET events from endpoints are sent to and indexed by Splunk, one may write queries to analyze the logs. Some important information from the EMET event is not automatically put into a field by Splunk. A field is a name/value pair that is searchable in Splunk.[8] Specifying new fields such as the module or employed mitigation may be helpful in analysis. Splunk allows for the creation of new fields using either manually defined regular expressions or a graphical tool that will construct regular expressions for you. Extracting fields allows for the creation of correlated searches. Here are a few example custom field extractions for EMET:

- Extract the executable blocked by EMET to a field named *EMET_EXE*:
  (?ms)close the application:\s+(?<EMET_EXE>\V+)

- Extract the individual mitigation EMET employed to a field named *EMET_Mitigation*:
  <Message>.*detected(?<EMET_Mitigation>.*) mitigation

- Extract the user whose application was blocked to a field named *EMET_User:*
  Name\s+:\s+YOURDOMAIN\S(?<EMET_User>\V+)

Leveraging those custom fields, queries will provide information about EMET activity on endpoints. Note that the queries below leverage custom fields created earlier.

All Mitigations:
host=COLLECTIONSERVER sourcetype="XmlWinEventLog:ForwardedEvents" Name="'EMET'" | Table _time, Computer, EMET_EXE, EMET_User | sort -_time

Mitigations Per Application with Sparkline:
host=COLLECTIONSERVER sourcetype="XmlWinEventLog:ForwardedEvents" Name="'EMET'" | stats sparkline count by EMET_EXE | sort –count

EMET_EXE ⇅	sparkline ⇅	count ⇅
OUTLOOK.EXE	⟋⋀	10
IEXPLORE.EXE	⟋Ⱳ	2
EXCEL.EXE	⟋⋀	1
POWERPNT.EXE	⟋⋀	1

Figure 1:   Mitigations Per Application with Sparkline

---

8   See http://docs.splunk.com/Splexicon:Field

Blocks per Mitigations as bar chart:
host=COLLECTIONSERVER sourcetype="XmlWinEventLog:ForwardedEvents" Name="'EMET'" | chart
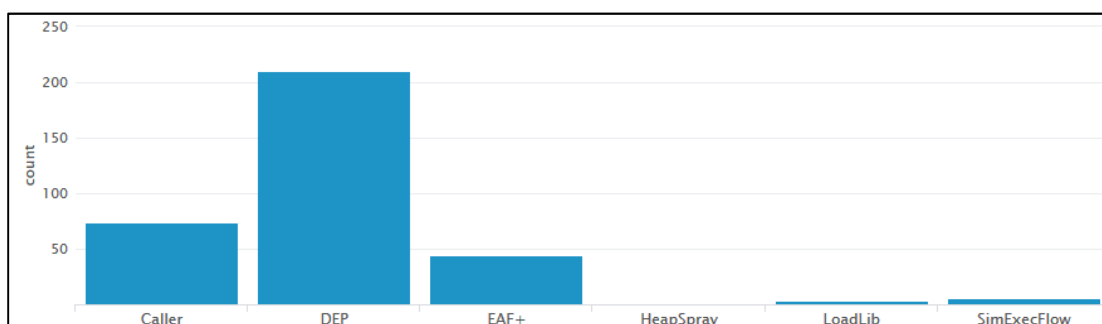count by EMET_Mitigation

Figure 2: Blocks per Mitigation as Bar Chart

4.4 Analyzing the Events

Analysis of the EMET events happening across an enterprise may help network defenders discover trends or correlations not evident through analyzing atomic incidents. By reviewing events across endpoints and users—and viewing those over time—defenders may gain practical insights. Consider the examples provided in Sections 4.4.1-4.4.3.

4.4.1   Example 1: Similar EMET Alerts for Individuals Across Departments

In a short period of time, the systems used by a number of individuals across departments generate similar EMET mitigation events. A correlation search of the individuals shows that they all received the same email with an attachment. The defender then pivots to search for other individuals who received that same email. The network defender can then examine the attachment of the email for malicious content, possibly removing it from any recipients who have not yet opened it or investigating if they have taken any other action (e.g., opening the attachment from a system that is not managed by the IT department or forwarding it outside the organization) and responding appropriately. The recipients of this email campaign may be part of past or future campaigns, so the defender can search for past (potentially missed) campaigns sent to these recipients or create a proactive alert when this collection of cross-department individuals receive messages in the future. Investigations of any relationships (e.g., publications, conference or training attendance, geography/travel) or non-relationships (i.e., there appears to be no correlation between these individuals) may be useful intelligence for defenders.

4.4.2   Example 2: EMET Outlier

The computers used by one employee may show up more frequently than average for EMET blocks of various types. This may indicate that the individual is being targeted or has unsafe computing practices. Additional training may be warranted for this individual (after an interview) such as recommended data handling practices or phishing awareness and social engineering resistance. Network defenders may also wish to examine the web or social media presence of this potentially targeted employee. Are they published or known to work with certain products or technologies?

Are they close co-workers with organizational leadership? Is the individual commonly being targeted with zero-days or attacks on specific software? Knowing the answers to those questions may provide additional intelligence to benefit network defenders. These data—both technical exploit techniques and meta-information—may also be helpful in understanding adversary capabilities and infrastructure if using the Diamond Model [Caltagirone 2013] as part of an overall defensive strategy.

4.4.3   Example 3: Sudden and Widespread Spike in EMET Mitigations

A sudden spike occurs in a particular application for a single EMET mitigation type. This may indicate that a widespread attack is happening on a commonly used application. However, it may also indicate that there is an incompatibility with some recently updated application widely used within a department or the organization at large. Remember that not every EMET alert indicates malicious activity, so it is possible that a software or configuration change has resulted in an unexpected rise in EMET mitigations. This may provide useful feedback for IT operations staff regarding enterprise practices related to change management, software deployment, and the like.

5 Conclusion

Tools like the Enhanced Mitigation Experience Toolkit from Microsoft can serve as an important layer of protection for enterprise endpoints. However, for the benefit of the overall security posture, information about EMET activities on those endpoints must be collected and analyzed to contribute to a continuous cycle of defensive activities.

By implementing a log collection and analysis strategy, network defenders can understand what is happening on endpoints through automation rather than relying on manual reporting methods.

References

URLs are valid as of the publication date of this document.

[Caltagirone 2013]
Caltagirone, S.; Pendergast, A.; & Betz, C. *The Diamond Model of Intrusion Analysis*. 2013. https://www.threatconnect.com/wp-content/uploads/ThreatConnect-The-Diamond-Model-of-Intrusion-Analysis.pdf

[Hutchins 2010]
Hutchins, E.; Cloppert, M.; & Amin, R. *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*. Lockheed Martin Corporation. 2013. http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
(Leave Blank)	August 2016	Final

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
Creating Centralized Reporting for Microsoft Host Protection Technologies: The Enhanced Mitigation Experience Toolkit (EMET)	FA8721-05-C-0003

6. AUTHOR(S)

Craig Lewis

Joseph Tammariello

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	CMU/SEI-2016-TN-007

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITORING AGENCY REPORT NUMBER
AFLCMC/PZE/Hanscom Enterprise Acquisition Division 20 Schilling Circle Building 1305 Hanscom AFB, MA 01731-2116	n/a

11. SUPPLEMENTARY NOTES

12A DISTRIBUTION/AVAILABILITY STATEMENT	12B DISTRIBUTION CODE
Unclassified/Unlimited, DTIC, NTIS	

13. ABSTRACT (MAXIMUM 200 WORDS)

Host protection strategies, such as enabling anti-exploitation features, can be effective in protecting Windows endpoints from compromise. Microsoft offers a tool to assist in this area and is provided at no cost. The Enhanced Mitigation Experience Toolkit (EMET) is a utility that helps to prevent the exploitation of software vulnerabilities.

EMET can be effective in safeguarding organizations from compromise by malicious actors. The configuration of EMET can be controlled centrally by enterprise system administrators using Group Policy. While centralized management capability is built into the tool, centralized reporting capabilities are not, creating a challenge when it comes to real-time situational awareness, metrics gathering, troubleshooting, and reporting. This report presents methods by which systems administrators and/or information security personnel can create a centralized reporting console using native Windows capabilities and the Splunk machine data analysis engine.

14. SUBJECT TERMS	15. NUMBER OF PAGES
host protection strategies, endpoints, EMET	19

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL